WHITE PAPER

VERITAS™

VERITAS StorageCentral™ - Permissions

ROLE BASED ACCESS CONTROL

TABLE OF CONTENTS

TABLE OF CONTENTS 2
introduction 3
Standard SRM Management 3
User/Group Rights 3
User/Group Permissions 4
DCOM Permissions 5
File System Permissions 6
Share Permissions 7
Registry/Active Directory Permissions 7
User Group Object Permissions 7
Advanced StorageCentral Management 8
Installation 8
Registry/Active Directory Permissions 8
Service Account 9
DCOM Identity 9
Recommendations 11
SC Permissions Addendum 12

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.

INTRODUCTION

Storage Resource Management (SRM); the creation of storage policies, the application of storage policies to managed object, the creation of detailed file system reports and the execution of those reports, in its entirety, should be limited to computer users with an understanding of the effects SRM may have on business continuity and system performance. To control who may create and apply policies, specific user rights, permissions to file system object, registry entries and Active Directory objects are required that typically necessitate administrative control.

This is especially true in the configuration, setup and implementation phases of SRM initiatives. Once SRM policies are created and administrative and user reports are created, on-going maintenance of managed objects and report execution may be delegated to users without full administrative rights. In the context of a helpdesk group, this paper focuses on the required permissions and privileges to perform SRM tasks utilizing StorageCentral. The following functions are discussed:

- Standard Management
  - Managing Space Allocation Objects
  - Managing File Blocking Objects
  - Executing Reports
- Advanced Management
  - Creating/Modifying SRM Policies
  - Creating/Modifying SRM Reports

STANDARD MANAGEMENT

Standard management would include functions such as modifying space allocation and file blocking objects and executing reports. To protect against anyone being able to modify objects, StorageCentral looks for required user privileges. Additionally, the architecture of the product requires permissions to various objects. These rights and permissions can be granted to individual users or a group, such as “Help Desk”. These rights and permissions are detailed below.

User/Group Rights

A “Help Desk” account requires: "Increase Quotas".

Start>Setup>Control Panel>Administrative Tools>Local Security Policy.
Double click "User Rights Assignment" and assign to the appropriate group or user.

This is a requirement for modifying or creating a space allocation object. StorageCentral services perform a function called “Service Impersonation.” This means that the StorageCentral Server Service will take on the security mask of the interactive user running the UI while setting a space allocation.

StorageCentral Server Service Account requires: “Increase Quotas”.

Start>Setup>Control Panel>Administrative Tools>Local Security Policy.
Double click "User Rights Assignment" and assign to the Service Account.

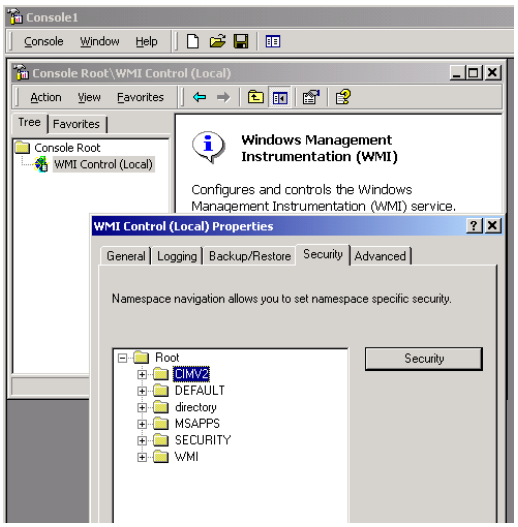
Due to the auto-detect feature included with StorageCentral, the service account at times does not have a interactive user to impersonate. This means the service account should also have the “Increase Quotas” right.

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.

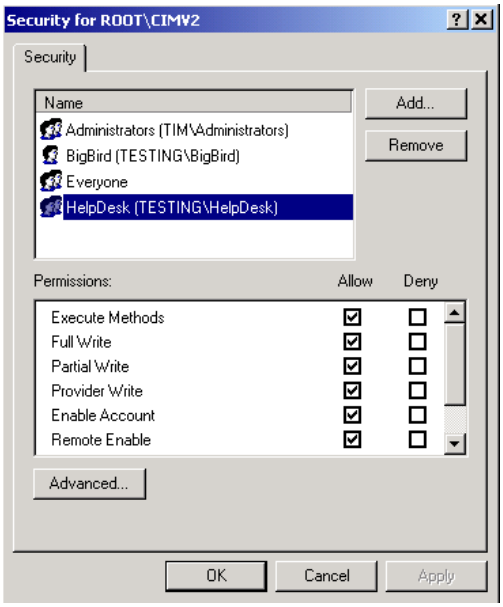
User/Group Permissions

WMI Permissions

Windows Management Instrumentation (WMI) is used by the wizards in the StorageCentral user interface to enumerate folders that policies may be applied. In order to be successful, the user running the UI on a client machine must be added to the security for CIMV2 WMI Control.

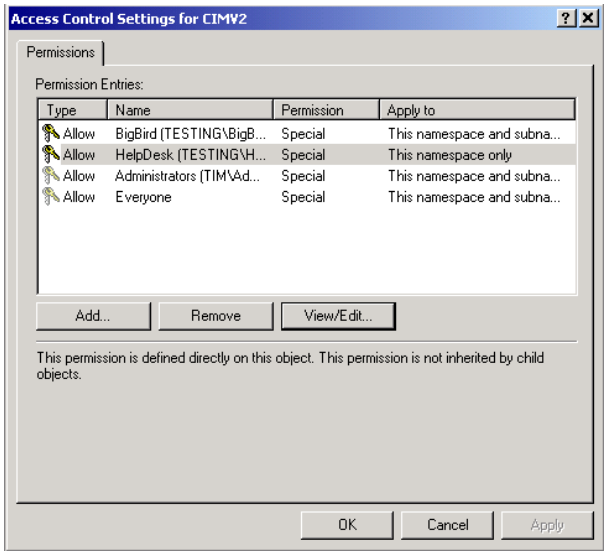


1) From an MMC console add WMI Control

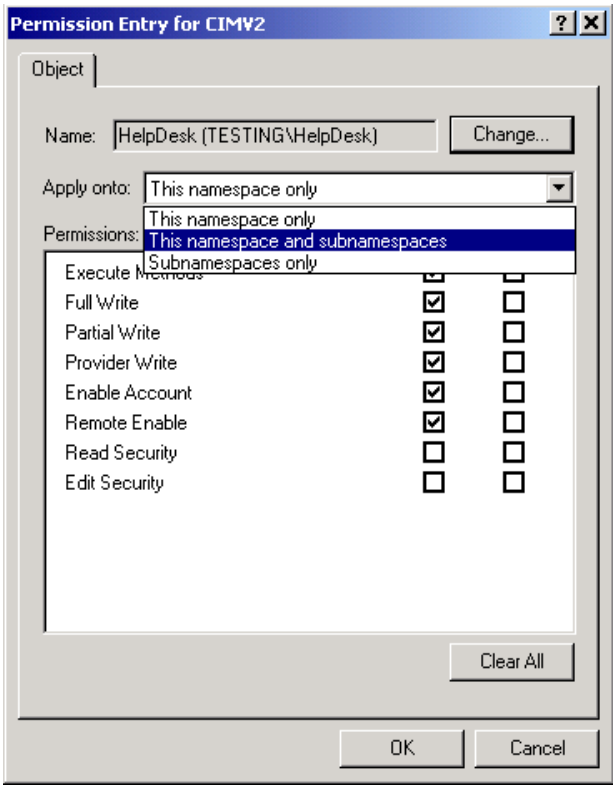


2) Click Security and add the specific user or group and allow access.

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.



3) Click the Advanced button and highlight the newly added user or group



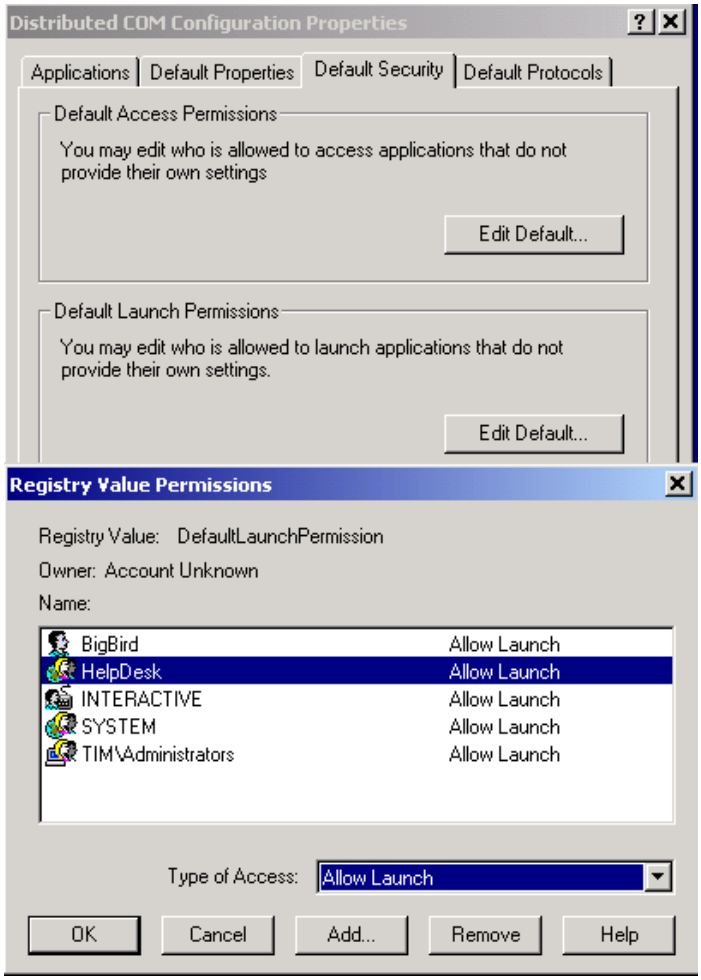
4) Click View/Edit and ensure the permissions are applied to 'This namespace and subnamespaces.'

The requirement to adding users and groups to the security for CIMV2 WMI Control can be bypassed by loading the Explorer Snapin for StorageCentral onto helpdesk client machines, and creating or modifying managed objects through Explorer. The reason this works is because the folder name is enumerated by Explorer and the snapin places you in the wizard beyond selecting the folder.

DCOM Permissions

Distributed Component Object Model (DCOM) is used by StorageCentral for client server communications. Specifically, when a report is launched from a client, a DCOM Server on the server is launched. This requires that the user running the report have DCOM launch permissions. This is granted in the DCOMCNFG utility as shown below.

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.



A DCOM server is launched when a report is executed from the GUI, in batch or from the drill-down feature of the StorageCentral Active reports.

File System Permissions

In order to create or modify a managed object the following is required:

- MODIFY permission to the root folder of each volume. The object and policy databases are stored there. This is because the QAPolicy database resides in the root of each partition and must be written to. When writing to this Access database file, the file is opened for shared access and Access creates a lock (.ldb) file. This create requires change permissions.
- LIST permission to all managed object directories (i.e. \Users). This is required to create a handle to the folder object in order to apply a policy.

In order to execute a report the following is required:

- LIST permission to the folder against which the report is being executed. Read permissions if the report is to return file ownership information. Though the report may not fail, it may be returned blank or not include a list of all files that meet the report query criteria.
- LIST permission to the StorageCentral folder typically located under C:\Program Files\WQuinn

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.

- READ/WRITE permissions to the StorageCentral installation folder \Reports on the Report collector, typically located under C:\Program Files\WQuinn\StorageCentral SRM\5.0\Reports. This is because when a report is executed an output file is created in this folder on the collector. This is true when reports are generated interactively as well.

    - This assumes that the WQRptSvr DCOM server on the collector is running under the Identity of Launching User. See section on DCOM Identity for alternatives.

- READ/WRITE permissions to the StorageCentral SRM installation folder \bin on the server where the report object exists. Typically, it is located under C:\Program Files\WQuinn\StorageCentral SRM\5.0\bin. This is required because the DCOM server on the target server generates a temporary file in this folder during report generation.

    - This assumes that the WQRptSvr DCOM server on the collector is running under the Identity of Launching User. See section on DCOM Identity for alternatives.

Share Permissions

StorageCentral reports require that a share be created called WQReportParameters and accessible with Modify permissions to users running reports. This share must reside on any StorageCentral Report Collector. By default, this share is created on folder C:\Program Files\WQuinn\StorageCentral SRM\5.0\Reports, with Everyone FULL access.

Registry/Active Directory Permissions

- READ permissions to the \WQuinn container within the Active Directory is required for a user or group to read the properties of a policy in order to apply those properties to a managed object. Likewise for report execution, the properties of the report set must be read from AD. This is true only for the Active Directory version of StorageCentral.
- READ permission to registry HKEY_LOCAL_MACHINE\Software\WQuinn and its sub keys. This is required for both report execution and applying a template policy to a managed object. The properties for both reports and policies are stored in the registry for the Standard version of StorageCentral.
- FULL permissions to HKLM/Software/WQuinn/StorageCentralSRM/5.0/Devices. This is required in both the Standard and Active Directory versions in order to create or modify File Blocking objects. The list of folders that have a blocking policy applied reside in this registry key.

User Group Object Permissions

A help desk account requires:

- FULL CONTROL permission to the Active Directory \WQuinn container. To edit this, run the ADSI (Active Directory Services Interface) MMC utility which can be installed from the \Support Tools directory of the Windows 2000 CD-ROM. To add this utility, choose Start>Run and type "MMC". In the MMC menu, choose "Console>Add/Remove Snapin". Click the ADD button. From the list choose ADSI. Click OK.

Log in as Administrator. In the ADSI editor, right click the root "ADSI" and choose "Connect". Click OK. Then expand the directory tree and select the \WQuinn container. Right click and choose Properties. Click the Security tab. Then click the Advanced button. Click the ADD button and select your help desk user or group. While they are selected, click the View/Edit button. In the "Apply Onto" box, select "This object and all child objects." Then click "FULL CONTROL" permission in the "Allow" column. Click OK 3 times until you have exited the security properties.

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.

ADVANCED MANAGEMENT

Advanced management would include functions such as installation, policy modification and creation, report definition and report set modification and creation and file group modification and creation. The sections below describe object permissions required to perform these advanced StorageCentral management functions.

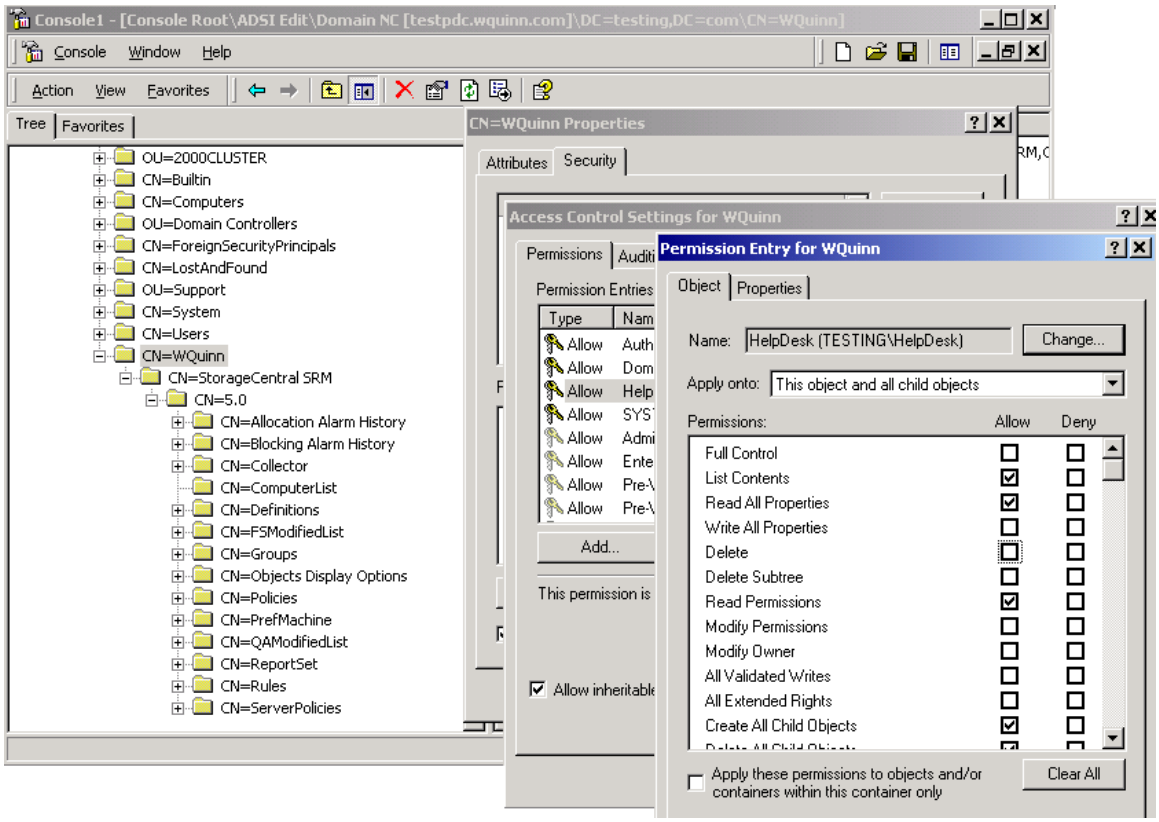
INSTALLATION

Installation should always be performed as a Domain Administrator as specified in the user manual. The Active Directory version requires special consideration as the schema needs to be extended and the policies need to be copied to the AD. These are typically one-time occurrences that occur upon the initial server install. However, subsequent AD versions server installations do require that the server be registered in the WQuinn Active Directory Container as installed servers. This will require that the user performing the install have access to the AD container CN=WQuinn/StorageCentral SRM/5.0/ComputerList. The User Guide should be referenced for more information on installation.

REGISTRY/ACTIVE DIRECTORY PERMISSIONS

The standard version of StorageCentral, non-AD, stores SRM policies, report definitions, report sets, file groups and preferred machines in the Registry under HKLM/Software/WQuinn/StorageCentral SRM/5.0. The Enterprise version of StorageCentral SRM, AD version, stores policies, report definitions, report sets, file groups and preferred machines in the Active Directory, by default, under CN=WQuinn/StorageCentral SRM/5.0/. These are all objects that a user who is responsible for modifying StorageCentral SRM configuration and management should have MODIFY (READ/WRITE) access. The AD version requires ADD and DELETE permissions on all child objects as the creation of a policy or report creates child objects. Following is a screen shot for setting AD permissions:

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.



SERVICE ACCOUNT

StorageCentral installs two services when the agent is installed. They are QuotaAdvisor Server and FileScreen Server. Like most services these may run under a specified account or as System. It is recommended that they run under a specified, administrative account that has the “Increase Quotas” right. If the System Account is used, certain features may not function, such as writing an event to a remote application log because this requires access to the network, which the local System account does not have.

DCOM IDENTITY

DCOM Servers can be configured using the utility DCOMCNFG. The StorageCentral DCOM Server to be considered is WQRptSvr. A process is launched for this server when the user interface is running, as well as on a Report collector when a report is launched. Keep in mind that the report collector may be the same machine as where the UI is running.

The WQRptSvr is responsible for running reports. When a report is submitted the WQRPTSVR, in turn, launches the WQFileSvr DCOM server on each server that hosts an object that the report is to be executed against. This means that much of the processing for report generation is distributed. Specifically, the file selection is distributed among the WQFileSvr processes on each server.

By default, the WQRptSvr DCOM server runs under the identity of the account you specified for the StorageCentral SRM services. This means that when a report is launched, it will run under the security mask of this account. This is very similar to a feature of the Task Scheduler. In Task Scheduler, you can schedule a job

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.

to run as another user. Basically, that is what occurs here. When the report is executed, it runs under the identity specified the DCOM Server WQRptSvr on the Report Collector.

If the WQRptSvr on the Report Collector is running as the Launching User, that means the report will execute as the user running the UI, or if the report is scheduled, as the user that the Task Scheduler is running as.

Specifying an account for the WQRptSvr is recommended. The WQRptSvr account must have enough permissions for accessing file system and using DCOM. This eliminates the need for the interactive user, or the task scheduler account to have access to the files the reports are executed against, the C:\Program Files\WQuinn\StorageCentral SRM\5.0\Reports folder and the C:\Program Files\WQuinn\StorageCentral SRM\5.0\bin folder. This is because the WQRptSvr DCOM Identity will have access to these folders.

The screen shot below shows you how to set this Identity in DCOMCNFG

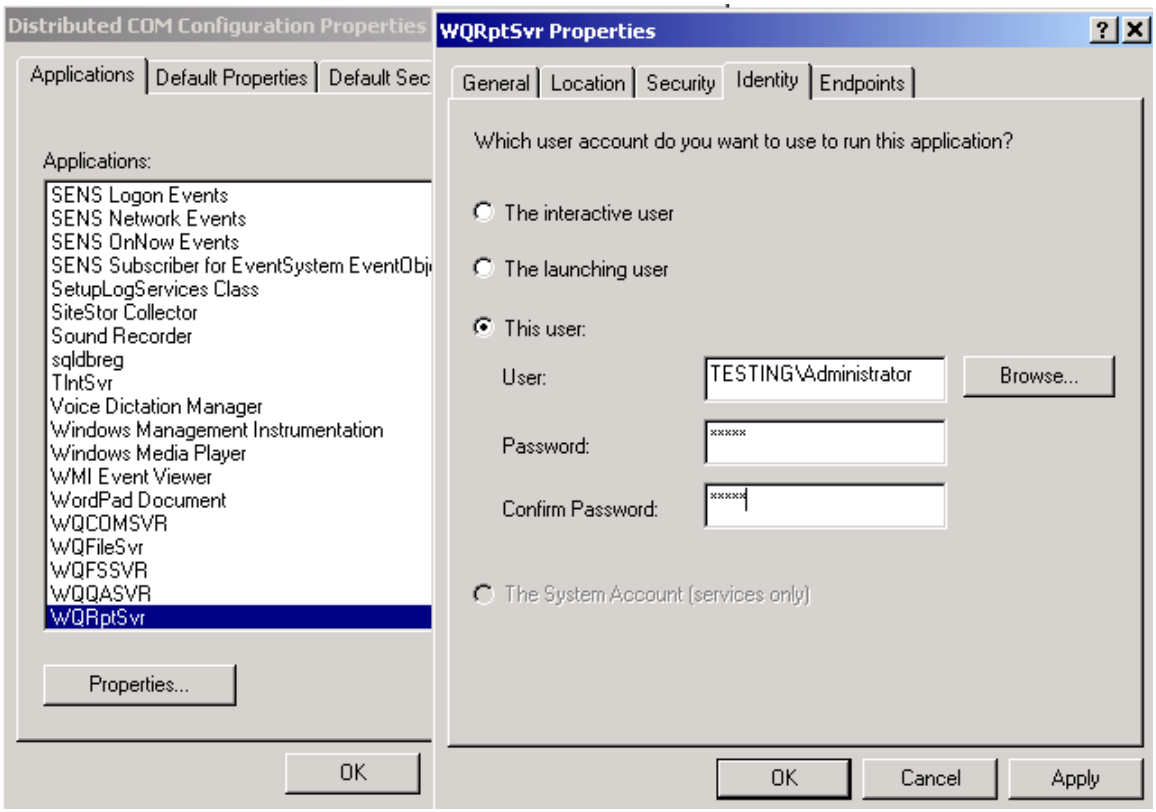
You may choose to set WQRptSvr to “launching user” if you wish to limit who will run reports. This must be done on the management console and the Report Collector(s) that the management station uses. These will likely be the same machine, but not necessarily. The permissions of the interactive user are used to generate reports. A user without permissions to the directories will encounter an access denied error or will be returned a blank or incomplete report, depending on where access was denied.

If WQRptSvr is set to “launching user”, you must change the AT service account for scheduled reports. To change it, go to the \WINNT\Tasks folder. From the menu choose Advanced>AT Service Account. You must stop and restart the Scheduler for this change to take effect.

When running the WQRptSVR as ‘Launching User’, reports will only include files, which the ‘Launching Users’, has LIST permissions to. A report will not display files for which you don't have LIST permission, or include the file size or type in your report totals. If you suspect that a report does not include all of the files in the object, verify that you have LIST permissions to all of the files. If a report is to return file ownership. READ access is required for the ‘Launching User’.

As stated earlier in the section, the WQFileSvr process actually does the file selection. As this DCOM server is launched by the WQRptSvr, the WQFileSvr identity should remain as ‘Launching User’. As the WQRptSvr Identity is always the launching user for this process, it will dictate who this process runs as.

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.



RECOMMENDATIONS

Perform Storage Resource Management functions under an administrative account. If not desirable, provide Storage Managers with access to

For Standard Edition, you need:

- READ/WRITE permissions to access local registry key [HKEY_LOCAL_MACHINE\SOFTWARE\WQuinn\] and its sub keys.
- LIST permissions to all folders that either reports will be executed against or space allocation will be applied.
- The Launching User for WQRptSvr should be an administrative account with access to C:\Program Files\WQuinn\StorageCentral SRM\5.0\bin and C:\Program Files\WQuinn\StorageCentral SRM\5.0\reports

For Active Directory edition, you need:

- The above recommendations for the Standard Edition
- READ/WRITE and ADD and DELETE all child objects permissions to the Active Directory \WQuinn container.

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.

STORAGECENTRAL PERMISSIONS ADDENDUM

A help desk user needs the following permissions for running StorageCentral reports on management station/Collector

Read & Execute, List folder contents, Read, Write permission to the \Program Files\ Internet Explorer directory and its sub directories.

Read & Execute, List folder contents, Read, Write permission to the \Program Files\Wquinn\StorageCentral\5.0 directory and its sub directories.

On Remote computer the following permissions are required.

Read & Execute, List folder contents, Read, Write permission to the \Program Files\Wquinn\ StorageCentral\5.0 directory and its sub directories.

DCOM (dcomcnfg) permission to launch application.(Log in as administrator, “RUN” “dcomcnfg”.Select “Default Security” then go to “Default Launch Permissions” select “Edit Default” add user or group and give “Allow Launch” access.

Configure WMI CIMV2 (wmimgmt) permission to allow “Remote Enable” apply on this name space and sub name space.(Log in as administrator, “RUN” “wmimgmt.msc”. Right click on “WMI Control (local)” and choose properties then select “security” expand “Root”, select CIMV2 and then select “ Security” add user or group and give allow “Remote Enable” permissions. Select “Advanced” then select user or group, click on “View/Edit” and select “Apply onto This namespace and subnamespace”.

WMI CIMV2 permissions are only required for users that will use the StorageCentral user interface to run reports. A report can also be executed by a user from the Active X drill-down feature of a summary report. For example, a summary report can be sent to a user that includes a line item for large files. If the user clicks the large files entry, a subsequent report will be launched. In this case, the user does not need to access the StorageCentral SRM user interface.

Note: READ permissions are required to all drives and directories that will be reported on. A report will not show files for which the user or group don’t have read permissions.

The WQRptSvr account must have enough permissions for assessing file system and using DCOM (A domain admin account is recommended).

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Specifications and product offerings subject to change without notice.